DRAFT: 3/24/10

Preliminary/Framing Comments

- Privacy and security protections are integral parts of the foundation for achieving meaningful use of health IT.
- A comprehensive set of privacy and security protections that build on current law and more specifically implement the principles in the Nationwide Data Sharing Framework is critical to building the "Trust Framework" that will support and enable meaningful use by clinicians and consumers.
- Fleshing out the details of these protections will be an ongoing focus of the workgroup.
- Today our recommendations focus on consent, which is just one element of a comprehensive framework of protections for electronic exchange of personal health data.

Recommendation

- When an EP or Hospital is engaging in direct, one-to-one exchange to meet the Stage 1 criteria for meaningful use, no additional consent/authorization requirements should be imposed beyond those that otherwise apply under state or federal law.
    - Assumes a direct exchange model without an intermediary such as an HIE or RHIO to facilitate the exchange – or if the exchange is facilitated by an intermediary such as an HIE or RHIO, the intermediary is merely facilitating the transfer of the data to the intended recipient and is not retaining individually-identifiable health information or accessing it beyond what is needed to facilitate the transport.
    - NHIN Direct is a project intended to draft specifications and services that address such one-to-one exchange.

- A priority requirement for Certified EHR Technology should include technical features that assist providers and hospitals in managing consent laws and patient preferences.

- Workgroup will focus next on whether additional consent requirements should apply when an intermediary or network is used and where that intermediary retains individually identifiable health information and/or has or provides greater access to the data than what is needed to facilitate the one-to-one transport.

Rationale

- Existing federal and state laws provide individuals/patients with some protections for identifiable health information, including the right to consent, authorize, or restrict access, use and disclosure of personal health information in certain circumstances.
- Providers/Hospitals are still required to navigate privacy rules (including rules regarding sensitive data) and patient requested preferences.
- In direct exchange, decisions about whether data is exchanged (and if so, how much) remain with the trusted holder of the data, who has the closest relationship to the patient and can be held accountable both by the patient and legal authorities.
- In many cases, such exchanges are consistent with patient expectations and arguably consent is implied. (For example, when patient is being referred to a specialist, referring physician can let the patient know that relevant health information for his or her care is being sent to the receiving provider.)
- Just applies to eligible providers and hospitals for Stage 1 of Meaningful Use. Meaningful use Stage 1 criteria cover exchanges for treatment, care coordination, some administrative tasks, insurance eligibility, public health reporting, and quality reporting.
- NCVHS recommendations on consent have focused on exchange via the "NHIN," which at that time was understood to refer to a "network of networks" approach and not necessarily direct exchange.
- Imposing additional consent requirements just for meaningful use for direct one-to-one exchange could be disruptive to care processes and provides a disincentive to adopt Certified EHRs because it's an obligation imposed on EPs and Hospitals that doesn't apply to other covered entities.